A Complexity Reduction Method for Extended Min-Sum based Nonbinary LDPC Decoder

M Anbuselvi [#1], S Salivahanan [*2]

[#] Assistant Professor, Department of ECE, SSN college of engineering
Kalavakkam, Tamilnadu, India
[1] anbuselvim@ssn.edu.in
[*] Professor, Department of ECE, SSN college of engineering
Kalavakkam, Tamilnadu, India
[2] salivahanans@ssn.edu.in

***Abstract*—Nonbinary LDPC codes are a class of linear block codes having the performance closer to Shannon's limit. Codes defined over higher order of Galois field, have increased computation complexity and thereby it put forth the challenges in efficient hardware realization of the decoder. In this paper, modifications in the Non-binary LDPC decoder to obtain reduced configuration sets, aimed to reduce the decoding complexity is proposed. Configuration sets are the possible combinations of the message sets that are involved in the parity check equation of LDPC decoder. Min-sum algorithm based decoder is modelled with the specification of IEEE 802.11n standard, with the codelength of 648, rate ½ for GF (4) Galois field, over the AWGN channel. The mathematical formulation of the proposed complexity reduction methodology is presented. The decoding performance of reduced configuration sets is analyzed and it is found that the complexity is reduced by an average of 83%, with negligible degradation in performance in terms of bit error rate.**

Keyword- Linear block code, Iterative decoding, Non-binary LDPC decoder, Configuration Set, Min-Sum decoding algorithm

I. INTRODUCTION

Error correction coding (ECC) is the mean whereby errors can be identified based upon received information. Low Density Parity Check (LDPC) codes are used in emerging wireless communication technologies namely DVB-S2 and IEEE 802.11n and IEEE 802.11g. It is claimed that LDPC codes will be the choice for future standards, such as 5G, and later versions of WiMax etc. Gallager invented the LDPC code in 1962, which is superior in terms of decoding than turbo codes decoding [1]. In addition LDPC approaches the Shannon's theoretical limit of channel capacity [2]. By the work of David Mackay, LDPC's revisions in mathematical models are evolved [3]. Use of the LDPC codes on the wireless sensor network shows that the system can be more energy efficient, in addition to better reliability [4]. One of the design issues of LDPC decoding is to make a tradeoff between the performance and complexity. Recently research has been concentrated on reducing the algorithmic complexity with reasonable decoding performance. In [5], the complexity reduction of LDPC decoding using min-sum algorithm, for DVB-S2 standard is addressed. It proposes two different approaches for reducing the computation strength of the decoding algorithm. The Parity check matrix (PCM) for non-binary can be constructed similar to binary LDPC, with the elements of the Galois Field (GF) over q. The quasi-cyclic LDPC code is another variant of LDPC code where the PCM structure is formed by cyclic shift, and is represented by a sub matrix corresponding to each non-binary element [6]. In comparison to Non-binary LDPC codes, the binary LDPC code has the competing performance and complexity for large block lengths. However for the shorter block length, the performance of binary LDPC is poor [7]. Thus Non-binary LDPC codes are more suitable for shorter block length. It has been noted that about 0.3 dB reduction in bit error rate at SNR=1, for non-binary codes [8]. Various methodologies for the reduction of the configurations with respect to the decoding algorithm are proposed in [9]. Non-binary LDPC can also be used for multiple antennas systems where it has been shown that [10], throughput of 600 Mbits/s can be obtained with four transmit and four receive antennas. In this paper, a complexity reduction methodology for non-binary LDPC codes is proposed and complexity reduction is analysed for IEEE 802.11n wireless communication standard [11].

II. NONBINARY LDPC DECODER

The design of decoder in a Non-binary LDPC codes involves computations of check node processing and variable node processing. The channel probabilities for each symbol of GF (q), is an array of q x ζ, corresponding to the codeword ζ. The check node computation involves initially, the identification of possible configuration sets of the symbols of GF (q) with respect to the channel probabilities. The parity check matrix H

also defines the computation complexity of the check nodes and variable nodes. The number of configuration sets and the associated matrix computation decides the complexity of the decoder.

For a non-binary LDPC, the computation complexity of the Belief Propagation (BP) algorithm is O (q^2). In [12] Declercq elaborates on reducing the complexity of BP algorithm with the log domain analysis and proposes Extended Min-sum (EMS) algorithm and the decoder is less sensitive to quantization noise. The efficiency of the MS algorithm has been analyzed in the different domains, namely probability domain, log domain and Log-likelihood ratio (LLR) domain [13]. Some modifications to the EMS algorithm towards the complexity reduction are addressed in [14, 15]. The system block diagram for the Non-binary LDPC decoder is shown in Fig 1, which uses the Min-sum decoding algorithm. The parity check matrix structure is embossed with the available a posterior channel information to form the Q-matrix, which are the input values for the check node processing. The check node processing of the Q-matrix, the configuration sets are defined over the elements of GF (q). The Min-sum decoding algorithm estimates the codeword.

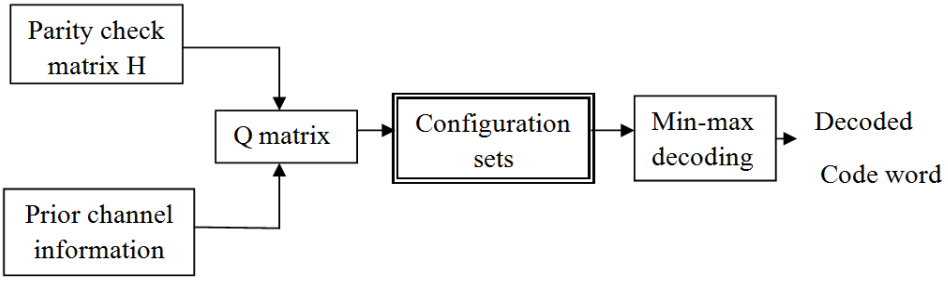

Fig. 1. System Block Diagram of Non-Binary LDPC Decoder

A. Min-sum Decoding

The mathematical model of the Min-sum decoding algorithm is as follows

Step 1: Initialization: Let $C_n(a)$ represents the a priori information of the nth symbol from the channel. $Q_{mn}(a)$ are the channel log likelihood ratios, initially assigned for the computation to the variable node unit.

$$C_n(a) = \ln(\Pr(c_n = s_n \mid channel) / \Pr(c_n = a \mid channel)) \quad (1)$$

$$Q_{mn}(a) = C_n(a) \quad (2)$$

Step 2: Check node update: Let $R_{mn}(a)$ represents the message computed at the check node unit, with respect to a node a in the Tanner graph.

$$R_{mn}(a) = \min_{(a_{n'})_{n \in N(m)\setminus\{n\}} \in A_{mn}(a)} \left(\sum_{n \in N(m)\setminus\{n\}} Q_{mn}(a) \right) \quad (3)$$

$$A_{mn}(a) := \{ a_n . \mid h_{mn} a + \sum_{n \in N(m)\setminus\{n\}} h_{mn} a_{n'} \} \quad (4)$$

Step 3: Variable node update: From the check node update unit, the messages $R_{mn}(a)$ are passed to the variable node update unit for the estimation of codeword.

$$Q'_{mn}(a) = C_n(a) + \sum_{m' \in M(n)\setminus\{m\}} R_{m'n}(a) \quad (5)$$

$$Q'_{mn} = \min_{a \in GF(q)} Q'_{mn}(a) \quad (6)$$

$$Q_{mn}(a) = Q'_{mn}(a) - Q'_{mn} \quad (7)$$

Step 4: Tentative decoding: With the messages received from the check node update unit, the codeword is tentatively decoded for the each symbol as

$$Q_n(a) = L_n(a) + \sum_{m \in M(n)} R_{mn}(a) \quad (8)$$

$$\hat{c}_n = \arg\min(Q_n(a)) \quad (9)$$

$$C = [\hat{c}_0 \hat{c}_1 ..... \hat{c}_{N-1}] \tag{10}$$

Step 5: Decision: The tentatively decoded symbols are cross verified with the parity check matrix, to validate the decoded codeword using

$$CH^T = 0 \; or \; iter \leq \max\_iter \tag{11}$$

The flow diagram of the Min-Sum algorithm is presented in Fig 2 in which each step of the algorithm is depicted with the corresponding input and output variables. The variable node is updated with the prior channel information during the first iteration. From the next iteration, the computations for the variable node update are carried out with the inputs from the check node update unit. The validation of the codeword is performed in the decision block and the iteration count is verified. If the codeword is not valid, the number of iterations is increased for the next cycle of decoding procedure. If the maximum iteration is attained and the codeword is not validated, then decoding failure is declared. If the iteration bound is not reached, the cycle repeats.

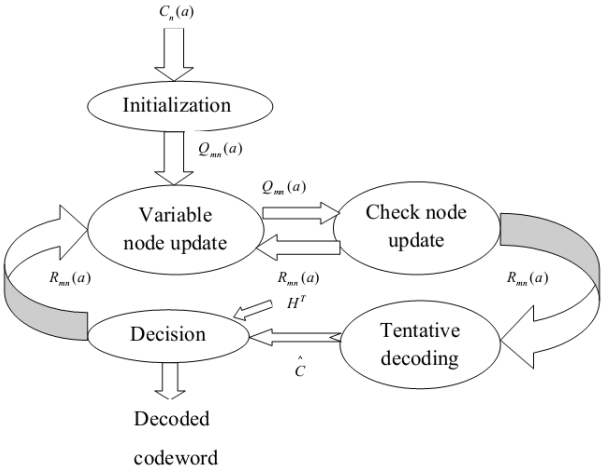

Fig. 2. Flow Diagram of Min-sum Algorithm

B. Performance Analysis

The analysis of the decoding performance of non-binary LDPC decoder using Min-sum algorithm is done with the Bit Error Rate (BER) graphs. It is compared with binary LDPC decoder of same specification. Fig 3 indicates that BER is better for the non-binary LDPC, when compared to binary LDPC coding. Simulation results found to agree with Hassani's [7] work on the comparison of binary and Non-binary LDPC codes. Simulations results also show that the decoding performance of Non-binary LDPC improves with the order of Galois field.

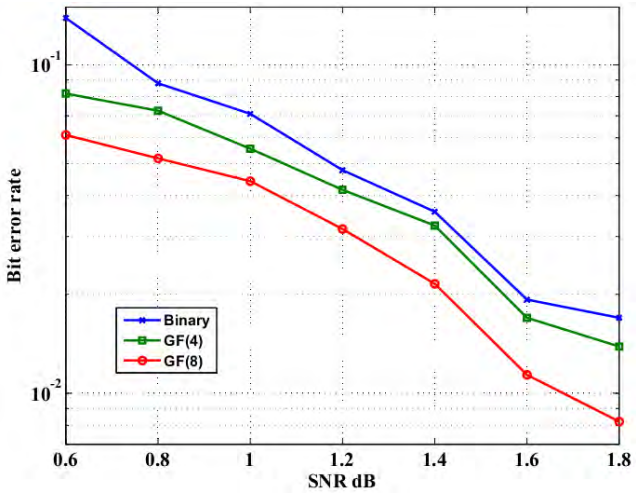

Fig. 3. Comparison of bit error rate for binary, GF (4) and GF (8) LDPC Codes

III. Formulation of Reduced Configuration Set

In this section, we propose a novel method of reducing the number of configurations to be verified at the parity check equations. We introduce a technique called variable threshold based configuration reduction. The flow of reducing the configuration set and the formation of M matrix are depicted in Figure 4. The configuration set block in the system diagram shown in Fig.1 can be replaced with this flow diagram

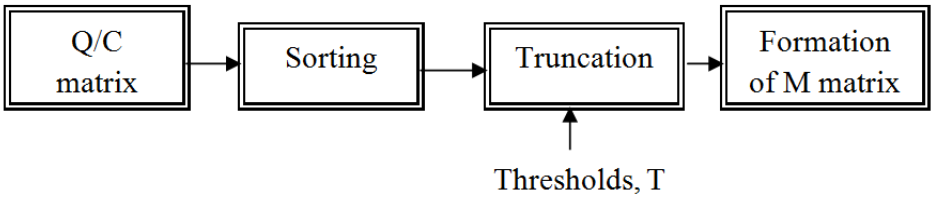

Fig. 4. Flow Diagram of Configuration Set Reduction

Notations used:

GF (q) = {0, 1. , q-1}, the Galois field with q elements, where q is a power of a prime number

l to denote the GF(q) symbols

S to denote the vectors of GF (q) symbols

H (m,n), the parity check matrix of the code

ζ, codeword set of the LDPC code

H (n), number of check nodes connected to the variable node n.

H (m), number of variable nodes connected to the check node m.

ξ (m), set of local configurations verifying the check node m with the linear constraint.

ξ(m|ln = l), local configuration sets, S verifying m, such that ln=l; given n ε H(m) and

l ε GF(q)

C_n, a prior channel information for the n[th] symbol

For a given GF (q), aprior information C having *l* columns and *q* rows is defined as,

$$C = \begin{bmatrix} C_1^{(0)} & C_2^{(0)} & \cdots & C_l^{(0)} \\ \vdots & \vdots & \cdots & \vdots \\ C_1^{(q-1)} & C_2^{(q-1)} & \cdots & C_l^{(q-1)} \end{bmatrix}$$

The Q-matrix is framed as follows. For each non-zero element in H-matrix, place the corresponding column vector from C. The elements that are placed should be permutated according to the symbol q. The partition of the Q matrix represents the likelihoods that the nth received symbol belonging to C.

$$Q = \left[\begin{array}{cc|cccc|c} C_1^{(0)} & C_2^{(0)} & \cdots & \cdots & \cdots & \cdots & C_n^{(0)} \\ \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ C_1^{(q-1)} & C_2^{(q-1)} & \cdots & \cdots & \cdots & \cdots & C_n^{(q-1)} \\ \hline \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \hline C_1^{(0)} & C_2^{(0)} & \cdots & \cdots & \cdots & \cdots & C_n^{(0)} \\ \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ C_1^{(q-1)} & C_2^{(q-1)} & \cdots & \cdots & \cdots & \cdots & C_n^{(q-1)} \end{array}\right]$$

The received probabilities of messages in C are arranged in descending order. First half of the values from the list are segregated and the thresholds are defined for framing the M matrix that contains reduced number of elements from C. The framing of reduced configuration set, ψ is given by the equation

$$\psi \equiv \{ \ C_n \in \ \xi \mid reduced\ configuration\ set \ \} \tag{12}$$

The range of thresholds, T is fixed to frame the M matrix. The formation of the M matrix is as follows.

$$M \equiv \{\, C_n \in T \mid Matrix\ of\ reduced\ configuration\ set \,\} \tag{13}$$

$$M = \left[\begin{array}{c|c|cccc|c} C_1^{(0)} & - & \cdots & \cdots & \cdots & \cdots & - \\ \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ - & C_2^{(q-1)} & \cdots & \cdots & \cdots & \cdots & C_n^{(q-1)} \\ \hline \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \hline C_1^{(0)} & - & \cdots & \cdots & \cdots & \cdots & C_n^{(0)} \\ \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ C_1^{(q-1)} & C_2^{(q-1)} & \cdots & \cdots & \cdots & \cdots & - \end{array}\right]$$

Consider a non-binary LDPC code with the code rate of ½, and (324,648) over GF (4). The LDPC code with these specifications has been followed in IEEE 802.11n standard. Let the channel probabilities for the codeword length of 6, are given as

$$C = \begin{bmatrix} 0.1825 & 0.1496 & 0.4449 & 0.0446 & 0.4123 & 0.3205 \\ 0.0461 & 0.7230 & 0.3241 & 0.0303 & 0.0735 & 0.0799 \\ 0.6157 & 0.0218 & 0.1335 & 0.5508 & 0.4362 & 0.4798 \\ 0.1555 & 0.1054 & 0.0972 & 0.3741 & 0.0778 & 0.1196 \end{bmatrix}$$

Let the parity check matrix defined over the GF (4) with the symbol set {0, 1, α, α2} be

$$H = \begin{bmatrix} \alpha & 0 & 1 & \alpha & 0 & 1 \\ \alpha^2 & \alpha & 0 & 1 & 1 & 0 \\ 0 & \alpha & \alpha^2 & 0 & \alpha^2 & 1 \end{bmatrix}$$

The permuted Q-matrix can be formed with the values of C and also according to the elements in H- matrix as follows,

$$Q = \left[\begin{array}{cc:c:cc:c} 0.1825 & 0 & 0.4449 & 0.0446 & 0 & 0.3205 \\ 0.1555 & 0 & 0.3241 & 0.3741 & 0 & 0.0799 \\ 0.0461 & 0 & 0.1335 & 0.0303 & 0 & 0.4798 \\ 0.6157 & 0 & 0.0972 & 0.5508 & 0 & 0.1196 \\ \hdashline 0.1825 & 0.1496 & 0 & 0.0446 & 0.4123 & 0 \\ 0.6157 & 0.1054 & 0 & 0.0303 & 0.0735 & 0 \\ 0.1555 & 0.7230 & 0 & 0.5508 & 0.4362 & 0 \\ 0.0461 & 0.0218 & 0 & 0.3741 & 0.0778 & 0 \\ \hdashline 0 & 0.1496 & 0.4449 & 0 & 0.4123 & 0.3205 \\ 0 & 0.1054 & 0.1335 & 0 & 0.4362 & 0.0799 \\ 0 & 0.7230 & 0.0972 & 0 & 0.0778 & 0.4798 \\ 0 & 0.0218 & 0.3241 & 0 & 0.0735 & 0.1196 \end{array}\right]$$

With the formulation of the reduced configuration set, the T-matrix can be given as follows

$$T = \begin{bmatrix} 0.1825 & 0.1496 & 0 & 0.0446 & 0 & 0 \\ 0.0461 & 0 & 0 & 0.0303 & 0.0735 & 0.0799 \\ 0 & 0.0218 & 0.1335 & 0 & 0 & 0 \\ 0.1555 & 0.1054 & 0.0972 & 0 & 0.0778 & 0.1196 \end{bmatrix}$$

With these range of values, defined as the threshold, the modified Q-matrix (called as M-matrix) can be given as

$$M = \left[\begin{array}{cccccc}
0.1825 & 0 & 0 & 0.0446 & 0 & 0 \\
0.1555 & 0 & 0 & 0 & 0 & 0.0799 \\
0.0461 & 0 & 0.1335 & 0.0303 & 0 & 0 \\
0 & 0 & 0.0972 & 0 & 0 & 0.1196 \\
\hline
0.1825 & 0.1496 & 0 & 0.0446 & 0 & 0 \\
0 & 0.1054 & 0 & 0.0303 & 0.0735 & 0 \\
0.1555 & 0 & 0 & 0 & 0 & 0 \\
0.0461 & 0.0218 & 0 & 0 & 0.0778 & 0 \\
\hline
0 & 0.1496 & 0 & 0 & 0 & 0 \\
0 & 0.1054 & 0.1335 & 0 & 0 & 0.0799 \\
0 & 0 & 0.0972 & 0 & 0.0778 & 0 \\
0 & 0.0218 & 0 & 0 & 0.0735 & 0.1196
\end{array}\right]$$

Hence, the computations on the check nodes are carried with this modified Q-matrix(or M-matrix) values

A. BER Analysis

With the proposed method of the configurations set reduction, the Min-sum decoding algorithm is analysed. The dependent parameter which decides on the reduction of configuration set is the threshold and its range. The threshold varies with respect to the channel probabilities, which in return depends on the SNR values. Therefore the variation in the SNR has the impact on the range of message probabilities and thereby the variable threshold range is fixed for the reduced configuration set. Hence the percentage of configuration reduction with the proposed algorithm varies as a function of SNR. The range of threshold is dynamically fixed based on the channel probabilities and for the SNR defined. Hence this method of decoding shows improvements on the decoding performance.

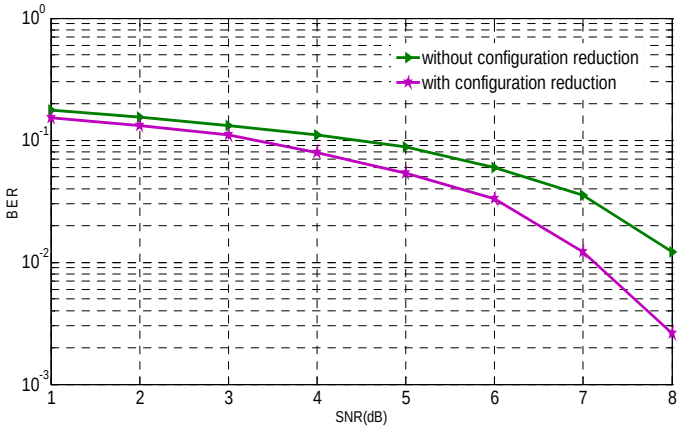

Fig.5 Performance comparison of Min-sum based LDPC decoder, without and with configuration reduction

The decoding performance of the Nonbinary LDPC decoder based on Min-sum algorithm, with and without configuration reduction technique is shown in figure 5. We infer that with the proposed configuration reduction method, the decoding performance is improved. The computation blocks involved in min-sum algorithm based nonbinary LDPC decoder are the comparison block and the adder block. The check node processing unit consists of a comparator and an adder for the min sum operation. As referred in the earlier section, the equation associated with check node unit, depicts the number of comparisons and additions with respect to the configuration set. In table I, the formulation of the computations using min-sum algorithm is presented.

TABLE I
Computation formulation for Min-sum algorithm

Computation block	Additions	Comparisons
CNU	$\Psi(n-k-1)w_r mq$	$(\Psi-1)w_r mq$
VNU	$\Psi(w_c-1)qn$	---

Where (n, m) represents the matrix size and (w_r, w_c) corresponds to the row and column weights respectively. 'q' is the order of Galois field and Ψ corresponds to the number of configurations defined. For the analysis, we took the values of these symbols as given in the case study. The reduced number of configurations for the different signal to noise ratio is presented in the table II below:

TABLE II
Reduced Number of Configurations

SNR (dB)	Configurations without reduction	Reduced number of configurations
0	1024	192
0.5		160
1		160
1.5		192
2		132

We infer from the table that the number of configurations being reduced is a function of signal to noise ratio. Also, the reduction in the configuration set is predominantly more, making this technique more attractive in terms of reduced computation complexity. The table III below shows the number of computations involved in both the check node processing unit and variable node processing unit. The calculations are done with respect to the equations given in the table I.

TABLE IIII
Number of Computations with and without Configuration Reduction

Number of configurations		Number of computations without configuration reduction			Number of computations with configuration reduction		
Without reduction	With reduction	CNU		VNU	CNU		VNU
		Addition	Comp.	Addition	Addition	Comp.	Addition
1024	192	73728	36828	24576	13824	6876	4608
	160				11520	5724	3840
	160				11520	5724	3840
	192				13824	6876	4608
	132				9504	4716	3168

From the above table, it is evident that the number of computations at the check node unit and variable node unit is greatly reduced. From the analysis of the computation reduction, with the technique of configuration reduction, we infer that in check node unit, on average 83.6% of additions and 83.7% of comparisons are reduced. Similarly in the variable node unit, there is 83.6% of addition reduction, on average in the variable node unit. It is clear that the contribution of this computation complexity reduction technique is dominant in the check node unit than in the variable node unit.

IV. CONCLUSION

In this paper, we have proposed modifications in the non-binary LDPC decoder algorithm to obtain the reduced configuration set. Simulations have been performed to analyze the efficiency of the reduced configuration set LDPC decoder, for the specification of IEEE 802.11n. The performance of the decoder is

found to reduce the complexity by 83% at a marginal degradation in the decoding performance. Further, the construction of the parity check matrix of the decoder can be varied, satisfying the row-column constraints, to improve the decoding performance.

REFERENCES

[1] R. G. Gallager, Low-Density Parity-Check Codes. Cambridge, MA: MIT Press, 1963.

[2] D.J.MacKay and R. Neal, "Near Shannon-limit performance of low density parity-check codes," IEEE vol. 32, pp. 1645–1646, 1996.

[3] M. Davey and D. MacKay, "Low-density parity-check codes over GF (q)," IEEE Communication Letter, vol. 2, no. 1, pp. 165–167, 1998.

[4] Mohammad Rakibul and Jinsang Kim, "On the Use of Low-density Parity Check code for Capacity and Bit Error Rate Sensitive Wireless Sensor Network at Nakagami-n channel", IETE Technical Review, vol.25, issue 5, pp. 277-284, 2008.

[5] Eun A Choi, Ji-Won Jung, Nae-Soo Kim and Deock-Gil Oh, "Complexity-Reduced algorithms for LDPC decoder for DVB-S2 systems", ETRI Journal, vol.27, no.5, 2005.

[6] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes, "Discrete Applied Mathematics, vol. 111, no. 1-2, pp. 122–175, 2001.

[7] El Hassani, S. Hamon, M. and H. Pénard, P. "Comparison Study of Binary and Non-Binary LDPC Codes Decoding," Proc in IEEE international conference, software, telecommunications and computer Networks(softCOM), pp.355 - 359A, 2010

[8] Rolando Antonio Carrasco, Martin Johnston, Non-binary Error Control Coding for Wireless Communication and Data Storage, John Wiley & Sons, ISBN 978-0-470-51819-9, 2009

[9] David Declereq, Marc Fossorier, " Extended Min sum algorithm for decoding LDPC codes over GF(q)", Information Theory, ISIT'05, 2005

[10] RonghuiPeng and Rong-Rong Chen, "Application of Nonbinary LDPC cycle codes to MIMO channels", IEEE transactions on Wireless Communications, vol.7, no.6, 2008

[11] IEEE 802.11 Wireless LANs WWiSE Proposal: High Throughput Extension to the 802.11 Standards, IEEE 2004.

[12] D. Declercq and M. Fossorier, "Decoding algorithms for non-binary LDPC codes over GF(q)" IEEE Trans. Communications, vol. 55, no. 4, pp. 633–643, 2007.

[13] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log- domain decoding of LDPC codes over GF (q)," in Proc. IEEE Int. Conf. Commun., Paris, France, pp. 772–776, 2004.

[14] Xinmiao Zhang and Fang Cai, "Reduced-complexity Extended Min-sum check node processing for Non-binary LDPC decoding", IEEE, pp.737-740, 2010

[15] Xiao Ma, Kai Zhang, Haiqiang Chen and BaomingBai, "Low complexity X-EMS algorithms for Non-binary LDPC codes", IEEE transactions on communications, vol.60, no.1, 2012.